

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **06-244833**

(43)Date of publication of application : 02.09.1994

(51)Int.Cl. H04L 9/32
H04M 3/42

(21)Application number : 03-220119

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 30.08.1991

(72)Inventor : NAKAJIMA SEIICHI
HARADA YONOSUKE
YOSHIDA MAKOTO

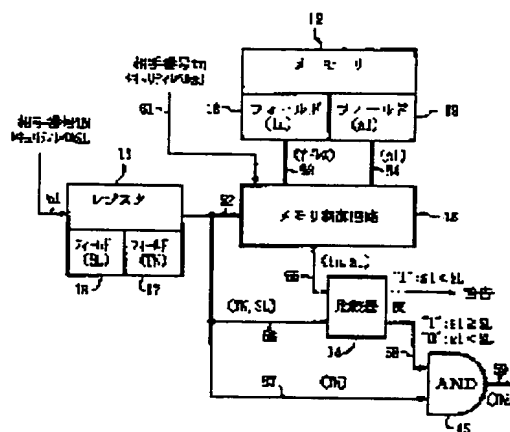
(54) COMMUNICATION SECURITY SYSTEM

(57)Abstract:

PURPOSE: To prevent the communication contents from being transferred to a communication opposite party from whom the content is kept a secret by a simple method by comparing the reception security level of the communication opposite party and the information security level on a transmission side and connecting the transmission side with the only communication opposite party having the reception security level which is higher than the information security level.

CONSTITUTION: The information security level SL stored in a field 16 is inputted in a comparator 14 via a control line 56, and a reception security level sl and an information security level SL are compared. In the case of (reception security level sl) \geq (information security level SL), the logic of a control line 58 becomes 1, the communication opposite party number TN stored in a field 17 via a control line 57 is inputted in an AND line 15 and the communication opposite party number TN is outputted to a control line 59 via the AND circuit 15.

The communication opposite party number TN outputted from the control line 59 is outputted to the central control unit, etc., of a communication network or an exchange and a communication is set.



LEGAL STATUS

[Date of request for examination] 27.08.1998

[Date of sending the examiner's decision of rejection] 20.08.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-244833

(43)公開日 平成6年(1994)9月2日

(51)Int.Cl.⁵

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/32

H 0 4 M 3/42

E

7117-5K

H 0 4 L 9/ 00

A

審査請求 未請求 請求項の数 1 O L (全 6 頁)

(21)出願番号 特願平3-220119

(22)出願日 平成3年(1991)8月30日

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(72)発明者 中島 誠一

東京都千代田区内幸町一丁目1番6号 日

本電信電話株式会社内

(72)発明者 原田 要之助

東京都千代田区内幸町一丁目1番6号 日

本電信電話株式会社内

(72)発明者 吉田 真

東京都千代田区内幸町一丁目1番6号 日

本電信電話株式会社内

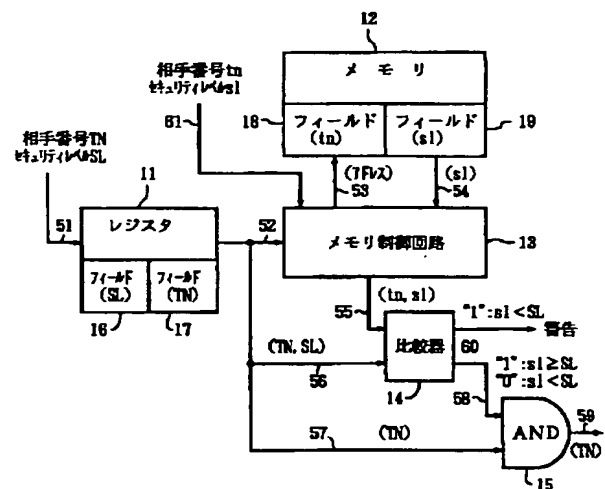
(74)代理人 弁理士 三好 秀和 (外1名)

(54)【発明の名称】 通信セキュリティ方式

(57)【要約】

【目的】 情報通信網において、簡単な方法により通信内容が秘密とすべき相手には転送されないようにすることが可能な通信セキュリティ方式の提供を目的とする。

【構成】 情報通信網における通信セキュリティ方式であって、予め通信相手に対応させた受信セキュリティレベルを設定して記憶しておき、通信する際に転送すべき情報に情報セキュリティレベルを設定し、通信開始時に通信相手の受信セキュリティレベルと転送すべき情報セキュリティレベルとを比較し、通信相手の受信セキュリティレベルが送信側の送信セキュリティレベル以上の場合にのみ通信を設定し、それ以外の場合には通信を設定しないように構成する。この方式は1対1の通信時にも、多対1の通信時にも適用でき、また、通信途中で情報セキュリティレベルを変えることもできる。



【特許請求の範囲】

【請求項1】 情報通信網における通信セキュリティ方式であって、

予め通信相手に対応させた第1のセキュリティレベルを設定して記憶しておき、通信する際に転送すべき情報に第2のセキュリティレベルを設定し、通信開始時に通信相手の第1のセキュリティレベルと転送すべき情報の第2のセキュリティレベルとを比較し、通信相手の第1のセキュリティレベルが送信側の第2のセキュリティレベル以上の場合にのみ通信を設定し、それ以外の場合には通信を設定しないことを特徴とする通信セキュリティ方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は通信セキュリティ方式に関し、特に、通信相手のセキュリティレベルと、転送すべき情報のセキュリティレベルに応じて、通信セキュリティを確保する通信セキュリティ方式に関するものである。

【0002】

【従来の技術】近年、社会の情報通信システムの発達により、通信が身近になっていつでも、誰とでも通信することが可能となってきている。例えば、電話網等を利用したファクシミリ通信の普及や、パーソナルコンピュータ等を利用したデータ通信の普及により、通信者は文字情報だけでなく、図形などのイメージ情報も送受信可能である。

【0003】しかしながら、一方では逆にこの便利さの影の部分も問題になってきている。従来の電話通信では、人間が直接介在するために、呼設定フェーズ後の通信フェーズにおいて通信相手を音声で確認してから通話を開始するため、誤ってダイヤルしても目的とする通信相手以外の第3者に通信内容が転送されることは防止できていた。ところが、ファクシミリ通信等の機械対機械の通信では、通信フェーズにおいて、通常、通信相手を確認しないため、誤ダイヤルをすると第3者に通信内容が転送されてしまうことになる。

【0004】ファクシミリ通信ではこのような誤ダイヤルを防止ため、従来は以下のような方法がとられていた。

【0005】1 まず、通信相手を呼出し、音声で相手を確認してからファクシミリ通信を開始するようにする。

【0006】2 同報通信を行う場合は、同報相手をあらかじめグループ化して誤りを防止する。

【0007】3 ファクシミリ信号を暗号化して送信する。

【0008】

【発明が解決しようとする課題】しかしながら、1の方法は、入手が介入するため繁雑になる問題がある。ま

た、ファクシミリ通信では同報通信を行うことが多々あり、多数の通信相手を指定するため必然的にダイヤル誤りの確率も高くなる問題もある。また、2の方法はグループの選択を誤り他の同報グループに通信内容が転送されてしまう恐れがある。更に、3の方法は端末機のコスト上昇、伝送効率の低下、端末での暗号／復号処理による転送時間の伸長等が問題になり、また、暗号／復号の鍵管理が繁雑になる問題もある。

【0009】本発明は上記事情に鑑みてなされたもので、その目的とするところは、簡単な方法により通信内容が秘密とすべき相手には転送されないようにすることが可能な通信セキュリティ方式を提供することにある。

【0010】

【課題を解決するための手段】前記目的を達成する本発明は情報通信網における通信セキュリティ方式であって、予め通信相手に対応させた第1のセキュリティレベル（受信セキュリティレベル）を設定して記憶しておき、通信する際に転送すべき情報に第2のセキュリティレベル（以降、情報セキュリティレベル）を設定し、通信開始時に通信相手の受信セキュリティレベルと転送すべき情報セキュリティレベルとを比較し、通信相手の受信セキュリティレベルが送信側の送信セキュリティレベル以上の場合にのみ通信を設定し、それ以外の場合には通信を設定しないことを特徴とするものである。

【0011】

【作用】本発明によれば、情報送信時に通信相手の受信セキュリティレベルと送信側の情報セキュリティレベルが比較され、情報セキュリティレベル以上の受信セキュリティレベルをもつ通信相手にのみ送信側が接続されるため、例えば通信相手を誤ってダイヤルしても接続されず、秘密がもれて問題となる相手に誤って情報が転送されることはなくなり、通信セキュリティを確保することができる。また、簡単な構成であるため、経済的な負担も少ない。

【0012】

【実施例】以下、本発明の実施例を図面に基づいて詳細に説明する。図1は本発明の通信セキュリティ方式の一実施例の構成を示すものであって、11はレジスタ、12はメモリ、13はメモリ制御回路、14は比較器、15はAND回路、16、17はレジスタ11のフィールド、18、19はメモリ12のフィールド、51、52、53、54、55、56、57、58、59、60、61は制御線を示している。

【0013】通信網のユーザが通信相手番号TNとその情報セキュリティレベルSL（SL=0、1、2……、Nで、数が多いほどセキュリティレベルが高いことを示す）を指定すると、これらの情報は制御線51を介してレジスタ11に入力され、通信相手番号TNはフィールド17に、情報セキュリティレベルSLはフィールド16に記憶される。通信相手番号TNが制御線52を介してメモリ制

御回路 13 に入力されると、メモリ制御回路 13 は制御線 53 を介して番地を指定し、メモリ 12 の内容を制御線 54 を介して順次読み出す。フィールド 18 には通信相手番号 tn が、フィールド 19 には受信セキュリティレベル sl ($sl=0, 1, 2, \dots, N$) が予め制御線 61 を介して設定されている。

【0014】メモリ制御回路 13 は、読み出されたフィールド 18 に記憶されていた通信相手番号 tn とレジスタ 11 から入力された通信相手番号 TN を比較し、一致した場合には制御線 55 にフィールド 19 に記憶されたこの通信相手番号 tn の受信セキュリティレベル sl を出力する。なお、通信相手番号 TN がフィールド 18 に存在しない場合には制御線 55 には最低のセキュリティレベルが出力される。フィールド 16 に記憶された情報セキュリティレベル SL は制御線 56 を介して比較器 14 に入力され、受信セキュリティレベル sl と情報セキュリティレベル SL とが比較される。

【0015】そして、(受信セキュリティレベル sl) \geq (情報セキュリティレベル SL) の場合には制御線 58 はの論理は“1”になり、制御線 57 を介してフィールド 17 に記憶された通信相手番号 TN が AND 回路 15 に入力され、通信相手番号 TN が AND 回路 15 を介して制御線 59 に出力される。制御線 59 から出力された通信相手番号 TN は通信網、あるいは交換機の中央制御装置等に送出されて通信が設定される。

【0016】一方、(受信セキュリティレベル sl) $<$ (情報セキュリティレベル SL) の場合には、制御線 58 の論理は“0”になり、制御線 59 には通信相手番号は出力されず、また制御線 60 の論理は“1”となる。制御線 60 の論理が“1”であることは、受信セキュリティレベル $sl <$ 情報セキュリティレベル SL であることを示し、ユーザに警告を発するものである。また、制御線 59 には通信相手番号が出力されないため、通信は拒絶される。

【0017】したがって、以上説明したように、受信セキュリティレベルが情報セキュリティレベル以上の場合にのみ通信が設定され、受信セキュリティレベルが情報セキュリティレベル未満の通信相手には通信が拒絶されるため、ユーザが転送すべき情報にセキュリティレベルを付加することにより、受信セキュリティレベルがそれ以下の相手には通信が拒絶され、セキュリティを確保することができる。

【0018】なお、図 1 の機構は端末に設置すること、通信網内、例えば、交換機に設置することも可能である。更に、端末に設置される場合には、例えば、制御線 59 の先は端末の選択信号送出回路等に接続され、制御線 60 は警告ランプ等を起動し、また、交換機に設置された場合には、例えば、制御線 59 は交換機の呼処理継続を起動し、また制御線 60 は呼損処理を起動することになる。

【0019】以上の説明では、通信相手が単数の場合で

あったが、1つの情報を複数の通信相手に転送する同報通信の場合においても本発明は適用できるものであり、この場合には、複数の通信相手に対応する受信セキュリティレベルについて情報セキュリティレベルとの比較を前述のように行い、(受信セキュリティレベル sl) \geq (情報セキュリティレベル SL) の通信相手にのみ通信を設定し、他の通信相手の通信は拒絶するように制御すればよい。

【0020】また、前述の説明ではファクシミリ通信を例にとって説明したが、本発明はファクシミリ通信に限定するものではなく、文書通信等の他の通信にも適用できることは明らかである。

【0021】更に、前述の説明では、呼の設定フェーズを例にとり説明したが、本発明は通信中においても適用することができる。例えば、会議電話、テレビ会議等において、特定の会話や画面を参加者のセキュリティレベルに応じて転送の制御をする必要が生じる場合がある。このような場合、参加者間におけるセキュリティが必要な会話や画面の転送の前に、前述と同様に情報セキュリティレベルを入力し、受信セキュリティレベルが情報セキュリティレベル以上の相手にのみ情報を転送することが可能になる。

【0022】図 2 はテレビ会議に本発明を適用した別の実施例を示すものであって、特定の参加者の端末装置の例を示すものである。図において、70 はメモリ、71 はレジスタ、72 はデコーダ、73、74 は AND 回路、75、76 はフリップフロップ (以降 F/F と記す)、77、78 は AND 回路、90 は情報線、91、92、93、94、95、96、97、98、99、100、101 は制御線である。また、図 1 と同じ構成の部材には同じ符号が付されており、13 はメモリ制御回路、14 は比較器、18、19 はメモリ 12 のフィールド、53、54、55、56、58、61 は制御線を示している。

【0023】なお、AND 回路 73 \rightarrow F/F 75 \rightarrow AND 回路 77 の経路はテレビ会議への各々の参加者に対応しており、制御線 98、99 等は参加者への伝送回路に接続されている。テレビ会議の冒頭には制御線 61 を介して参加者の受信セキュリティレベル sl がメモリ 70 に設定される。また、説明を簡単にするために参加者の番号とメモリ 70 のアドレスは一致するものとする。更に、テレビ会議の冒頭には制御線 100 を介して最も低い情報セキュリティレベル sm がレジスタ 71 に設定され、後にセキュリティが必要になった時にその時の参加者のレベルに応じた情報セキュリティレベル SL が設定される。

【0024】最も低い情報セキュリティレベル sm が設定されると、制御線 101 を介してメモリ制御回路 13 が起動される。制御線 53 にはアドレスが発生されメモリ 70 に設定された参加者各々の受信セキュリティレベル

slが制御線54を介して呼び出され、その値は制御線55に出力される。制御線56にはレジスタ71に入力された情報セキュリティレベルsmまたはSLが加わり、比較器14において、受信セキュリティレベルslと情報セキュリティレベルsmまたはSLが比較され、(受信セキュリティレベルsl) \geq (情報セキュリティレベルsmまたはSL) の場合には制御線58の論理は“1”になる。同時に制御線91に前述のアドレスが入力され、デコーダ72がこのアドレスをデコードし、例えば、制御線93が選択されて論理が“1”になる。制御線93と制御線58の論理積がAND回路73でとられ、制御線94の論理値にF/F75はセットされる。

【0025】従って、(参加者の受信セキュリティレベルsl) \geq (情報セキュリティレベルsmまたはSL) の場合にはその参加者に対応するF/F75等は論理が“1”に設定され、それ以外の場合にはF/F75等は論理が“0”に設定される。情報線90には会話や画像の符号化された情報が乗っており、AND回路77等で論理積がとられ、F/F75等の論理が“1”に設定された参加者のみに会話や画像情報が制御線98等に出力されることになる。メモリ制御回路13はすべての参加者のアドレスを発生し、F/F75等を所定の値に設定する。

【0026】前述のようにテレビ会議の冒頭では最も低い情報セキュリティレベルsmが設定されるため、最初はF/F75、76等はすべて論理が“1”に設定され、この端末からすべての参加者に会話や画像情報が転送されることになる。セキュリティが必要になった場合には、情報セキュリティレベルSLを制御線100を介して再設定すると、前述のようにすべての参加者について受信セキュリティレベルslと情報セキュリティレベルSLとが比較され、F/F75等を新たな値に再設定する。したがって、(受信セキュリティレベルsl) < (情報セキュリティレベルSL) の参加者のF/Fは論理が“0”に設定されるため、情報線90の情報はその参加者には転送されず、セキュリティが確保される。

【0027】情報セキュリティレベルSLを変更したいときには、任意の時点で制御線100を介して新たな情報セキュリティレベルSLを入力することにより、任意の所

要のセキュリティが確保できる。

【0028】

【発明の効果】以上説明したように本発明によれば、情報セキュリティレベル以上の受信セキュリティレベルをもつ通信相手にのみ通信が設定されるため、例えば、通信相手を誤ってダイヤルしても秘密がもれて問題となる相手には情報が転送されず、この結果、通信セキュリティを確保することができる。また、テレビ会議のような多対1の通信における通信フェーズにおいて、各々の通信情報のセキュリティレベルに応じて特定の通信相手にのみ情報を転送する等の制御も可能となる。

【0029】本発明では、従来の対策や方式のように人手が介入したり、端末が複雑になったり、転送時間が伸長する等の問題もなく、さらに簡単な構成であるため経済的な負担も少い特徴をもっている。

【図面の簡単な説明】

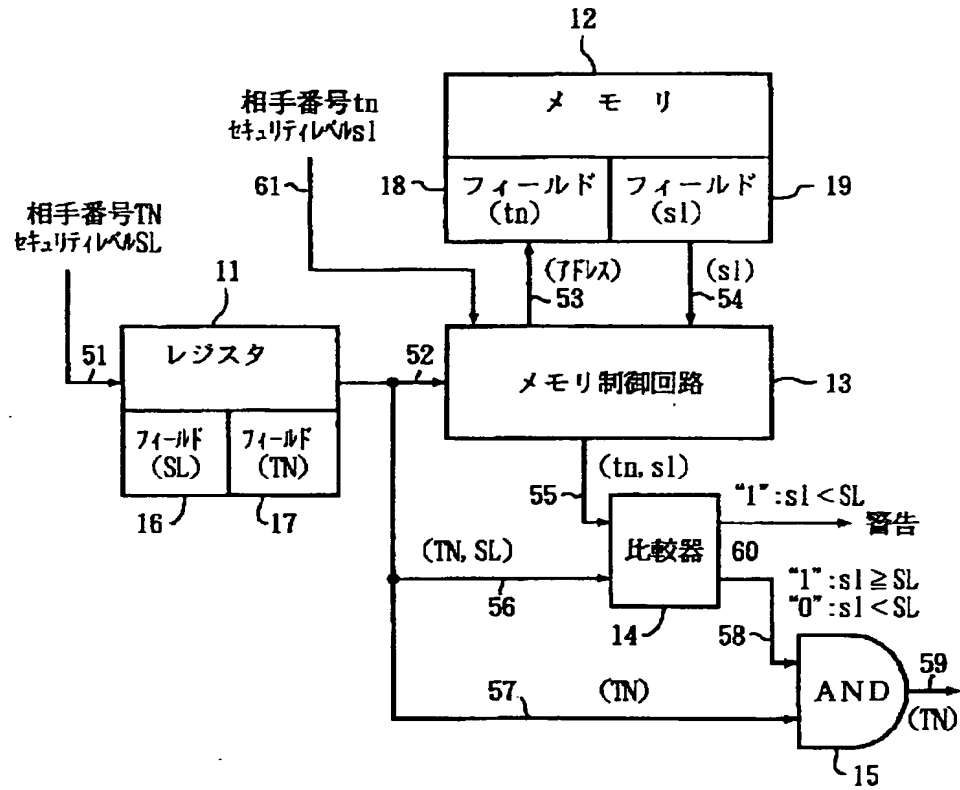
【図1】本発明の通信セキュリティ方式の一実施例を示すものである。

【図2】本発明の他の実施例を示すものである。

【符号の説明】

- 11 レジスタ
- 12 メモリ
- 13 メモリ制御回路
- 14 比較器
- 15 AND回路
- 16, 17 フィールド
- 18, 19 フィールド
- 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61 制御線
- 70 メモリ
- 71 レジスタ
- 72 デコーダ
- 73, 74 AND回路
- 75, 76 フリップフロップ
- 77, 78 AND回路
- 90 情報線
- 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101 制御線

【図1】



【図 2】

